VAIXUS
Technologies

VAIXUS-CS-003

Enterprise Email Security & Transport Assessment

A Laboratory-Engineered Consulting Simulation — Regulated Financial Services

Prepared for: Caldwell Harbor Trust (Synthetic Engagement)
Prepared by: Vaixus Technologies
Publication Date: July 20, 2026
Document Version: 1.0
Classification: Laboratory Simulation — Public Portfolio Use

LABORATORY-ENGINEERED CONSULTING SIMULATION

This report is a fictional, laboratory-generated case study prepared for portfolio and methodology-demonstration purposes. It does not describe a real client, a real organization, or an actual engagement.

Confidentiality Notice

This document is a laboratory-engineered consulting simulation produced by Vaixus Technologies for portfolio, training, and methodology-demonstration purposes. All organization names, personnel, domains, IP addresses, DNS records, SMTP transcripts, authentication results, and engineering findings contained within this document are entirely synthetic and were constructed within a controlled laboratory environment. No portion of this report describes, references, or was derived from any real organization's infrastructure, personnel, or confidential information.

This report does not represent an actual client engagement. Vaixus Technologies has not been retained by, and has no business relationship with, any organization resembling the fictional entity described herein. Any resemblance to an actual organization, domain, or individual is coincidental and unintended.

Where this document is distributed for evaluative purposes (e.g., prospective client discovery, recruiting, or partner review), it should be treated as a demonstration of Vaixus Technologies' consulting methodology, technical documentation standard, and analytical approach — not as evidence of prior client work or measured business outcomes.

If adapted as a template for an actual client engagement, all synthetic evidence contained in this document must be replaced in its entirety with verified production evidence before delivery, and this notice must be revised to reflect the real engagement's confidentiality requirements.

Document Control

Field	Value
Document Title	VAIXUS-CS-003 — Enterprise Email Security & Transport Assessment
Document Version	1.0
Publication Date	July 20, 2026
Prepared By	Vaixus Technologies
Review Status	Final — Approved for Portfolio Publication
Classification	Laboratory Simulation — Public Portfolio Use
Engagement Type	Laboratory-Engineered Consulting Simulation

Revision History

Version	Date	Author	Summary of Changes
0.1	July 6, 2026	Soorya S V	Initial discovery findings drafted following environment reconnaissance.
0.6	July 15, 2026	Soorya S V	Technical findings and remediation roadmap completed; internal engineering review.
1.0	July 20, 2026	Soorya S V	Final release following documentation and executive review.

Table of Contents

1. Executive Summary

Caldwell Harbor Trust (“Caldwell Harbor”), a regional trust bank headquartered in Portland, Maine, engaged Vaixus Technologies to conduct an independent assessment of its email transport security — the controls governing encryption-in-transit, DNS integrity, and delivery assurance for correspondence with correspondent banks, institutional trust clients, and regulatory counterparties. Unlike a general deliverability review, this engagement was scoped specifically at the request of Caldwell Harbor's Information Security Officer following an internal audit recommendation to independently verify the bank's DNSSEC, MTA-STS, and TLS reporting posture.

Caldwell Harbor's baseline sender authentication (SPF, DKIM, DMARC) is comparatively mature relative to the other environments in Vaixus's portfolio: DMARC is already enforced at p=reject, and DKIM and SPF are both correctly and narrowly scoped. This assessment's findings instead concentrate on the transport-security and DNS-integrity layer beneath that authentication posture — controls that are less commonly audited but equally consequential for an institution handling wire-transfer confirmations and trust correspondence.

Vaixus identified thirteen findings. Two are rated Critical: the domain's DNS zone is not protected by DNSSEC (no Delegation Signer record is published at the registrar despite signed records existing at the zone itself, leaving the chain of trust incomplete), and the bank's MTA-STS policy — which the Information Security team believed was actively enforcing encrypted delivery — has remained in “testing” mode since deployment and provides no actual protection against TLS downgrade or interception.

This assessment finds no evidence of active compromise or an exploited vulnerability. Every finding is a configuration or operational-maturity gap in controls that were correctly selected but not fully completed or monitored. Given Caldwell Harbor's regulated status and the correspondent-banking context in which these controls operate, Vaixus recommends prioritizing the two Critical findings ahead of the bank's next scheduled compliance review cycle.

Infrastructure Maturity Snapshot

Dimension	Current State	Target State
Sender Authentication (SPF/DKIM/DMARC)	Mature — DMARC enforced at p=reject	Maintain; add RUF for forensic detail (CS003-08)
DNS Integrity (DNSSEC)	Signed at zone; chain of trust incomplete (no DS record)	Full chain of trust validated end-to-end
Transport Security (MTA-STS/TLS-RPT)	Deployed in monitoring-only (testing) mode	MTA-STS enforced; TLS-RPT actively reviewed
Delivery Assurance (Reverse DNS)	Partial — 3 of 6 relay IPs lack PTR records	Full PTR coverage across all outbound relay IPs

2. Environment Overview

Caldwell Harbor Trust is a regional trust bank providing fiduciary, trust administration, and correspondent banking services, headquartered in Portland, Maine, with approximately 450 employees. As a regulated financial institution, Caldwell Harbor is subject to prudential supervisory oversight and maintains a formal information security program, including scheduled independent review of technical controls — the origin of this engagement.

Caldwell Harbor operates a hybrid mail architecture: Microsoft 365 (Exchange Online) serves as the primary corporate mailbox platform, with a dedicated on-premises Secure Mail Gateway handling compliance journaling (a regulatory recordkeeping requirement) and enforcing transport-layer security policy for correspondence with correspondent bank partners and institutional trust clients. All inbound and outbound correspondent-bank traffic is routed through this gateway rather than directly through Exchange Online.

Infrastructure Inventory

Component	Platform / Vendor	Function
Primary Domain	caldwellharbortrust.com	Corporate mail, brand identity, public DNS zone
Corporate Mail Platform	Microsoft 365 (Exchange Online)	Employee mailboxes
Secure Mail Gateway	On-Premises Hybrid Appliance	Compliance journaling; correspondent-bank TLS enforcement
Compliance Archive	On-Premises Journaling Store	Regulatory recordkeeping for correspondence
DNS Provider	Managed Authoritative DNS (registrar-hosted)	Public zone hosting for caldwellharbortrust.com
MTA-STS Policy Host	mta-sts.caldwellharbortrust.com	Published transport security policy
TLS-RPT Reporting	Configured, delivered to Secure Mail Gateway vendor mailbox	Aggregate TLS negotiation reporting

Figure 1 illustrates the relationship between Exchange Online, the Secure Mail Gateway, and Caldwell Harbor's correspondent-bank and institutional-client counterparties.

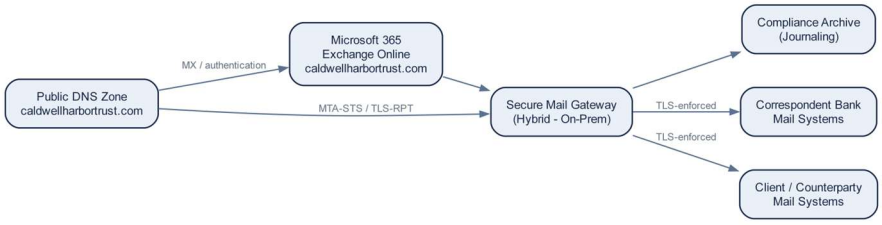

Figure 1 — Enterprise Mail Architecture

3. Assessment Scope

In Scope

- DNSSEC configuration and chain-of-trust validation for caldwellharbortrust.com
- MTA-STS policy configuration, mode, and cache lifetime
- TLS-RPT reporting configuration and organizational review process
- Reverse DNS (PTR) coverage for all outbound mail relay IP addresses
- Secure Mail Gateway STARTTLS negotiation and fallback behavior
- DKIM key rotation history and cadence
- DMARC reporting configuration (aggregate and forensic)
- Zone-level DNS hygiene (SOA parameters, legacy record references)

Out of Scope

- Core banking system security and transaction-processing controls
- Physical security of the compliance archive or data center
- Regulatory compliance certification or examination readiness (beyond the technical controls listed above)
- Endpoint security of employee workstations
- Mail content, e-discovery, or records-retention policy review
- Penetration testing of the Secure Mail Gateway appliance itself

This assessment is a technical review of transport-security and DNS-integrity controls. It does not constitute a regulatory examination, a penetration test, or a certification of compliance with any specific banking regulation.

4. Infrastructure Architecture

Caldwell Harbor's architecture separates two distinct trust boundaries: general corporate correspondence, handled entirely within Microsoft 365, and correspondent-bank and institutional-trust correspondence, which is routed through the on-premises Secure Mail Gateway specifically because that gateway enforces TLS policy and performs compliance journaling that Exchange Online alone does not provide for this use case.

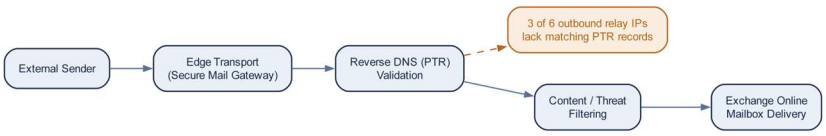

Figure 5 — Secure Mail Routing & PTR Validation

Figure 6 summarizes the full control inventory reviewed in this engagement, overlaid against Caldwell Harbor's stated trust boundary.

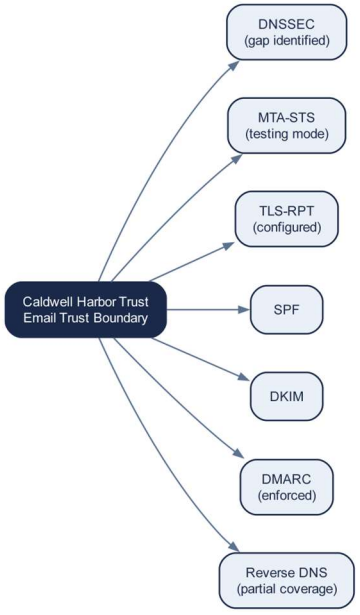

Figure 6 — Infrastructure Trust Relationships (Control Inventory)

5. Assessment Methodology

Vaixus applied its standard five-stage methodology, extended with transport-security-specific validation appropriate to a regulated financial institution.

- Discovery Workshop — structured interviews with the Information Security Officer and Network Operations to document intended controls, prior audit findings, and operational ownership.
- DNS and Trust-Chain Reconnaissance — authoritative-record enumeration and DNSSEC chain-of-trust validation (DS, DNSKEY, RRSIG) using recursive resolver validation testing.
- Transport Security Trace Testing — controlled SMTP sessions against Caldwell Harbor's inbound relay to observe actual STARTTLS negotiation and MTA-STS policy enforcement behavior, including simulated policy-fetch and fallback scenarios.
- Reverse DNS and Reputation Review — PTR record validation for every outbound relay IP address, cross-referenced against Secure Mail Gateway configuration.
- Findings Synthesis and Executive Readout — consolidation into severity-rated, business-impact-aligned recommendations presented to Caldwell Harbor's Information Security Officer and Chief Risk Officer.

All engineering evidence referenced in this report was captured during reconnaissance and trace-testing and is reproduced in the Technical Appendix.

6. Executive Findings Summary

Vaixus identified thirteen findings: two Critical, three High, five Medium, two Low, and one Informational.

ID	Finding	Category	Severity
CS003-01	DNSSEC chain of trust incomplete (no DS record at registrar)	DNS Integrity	Critical
CS003-02	MTA-STS policy remains in testing mode, not enforce	Transport Security	Critical
CS003-03	3 of 6 outbound relay IPs lack matching PTR records	Delivery Assurance	High
CS003-04	TLS-RPT reports generated but never reviewed	Operational Risk	High
CS003-05	Secure Mail Gateway falls back to plaintext on STARTTLS failure	Transport Security	High
CS003-06	DKIM key rotation overdue (unrotated 3+ years)	Authentication	Medium
CS003-07	MTA-STS max_age set long before policy validated in production	Transport Security	Medium
CS003-08	DMARC forensic reporting (RUF) not configured	Authentication	Medium
CS003-09	No documented incident-response runbook for authentication failures	Governance	Medium
CS003-10	Secure Mail Gateway outbound IP adjacency to flagged hosting range	Reputation Risk	Medium
CS003-11	SOA timing parameters are unreviewed legacy defaults	DNS Hygiene	Low
CS003-12	DNS TXT records reference bank's pre-rebrand legacy name	DNS Hygiene	Low
CS003-13	BIMI not implemented despite satisfied DMARC prerequisite	Security Best Practices	Informational

7. Detailed Technical Findings

Findings are presented in descending order of severity.

CS003-01 — DNSSEC Chain of Trust Incomplete — No DS Record at Registrar

Severity	Critical
Category	DNS Integrity
Reference	RFC 4033 §2; RFC 4035 §2.4

Evidence.

caldwellharbortrust.com publishes DNSKEY and RRSIG records at the zone itself, but no corresponding Delegation Signer (DS) record has been published at the parent (.com) zone through the domain's registrar, breaking the chain of trust required for DNSSEC validation.

```
$ dig DNSKEY caldwellharbortrust.com +short
257 3 13 (public key present — zone-signing key)
256 3 13 (public key present — key-signing key)
$ dig RRSIG caldwellharbortrust.com +short | head -1
SOA 13 2 3600 ... (signature present)
$ dig DS caldwellharbortrust.com +short
(no result — no DS record published at registrar)
$ delv @8.8.8.8 caldwellharbortrust.com
; resolution failed: insecure (no chain of trust)
```

Technical Analysis.

DNSSEC signing was evidently configured at the zone (DNSKEY and RRSIG records exist and are internally consistent) but the corresponding DS record was never submitted to the registrar to complete delegation signing at the parent zone. Without this step, validating resolvers cannot establish a chain of trust from the root down to caldwellharbortrust.com, and the zone is treated as unsigned (“Insecure”) by every validating resolver on the internet — identical in practice to having no DNSSEC at all, despite the signing infrastructure being technically present.

Business Impact.

This finding is the single most consequential item in this report because it undermines the integrity guarantee beneath every other control assessed here: SPF, DKIM, DMARC, and MTA-STS records are all retrieved via the same unvalidated DNS resolution path. A network-position attacker capable of DNS response manipulation could, in principle, forge any of these records for a validating resolver that believes it is receiving authentic data, since no resolver actually validates this zone today.

Recommendation.

Submit the zone's DS record to the domain registrar to complete delegation signing, and validate end-to-end chain-of-trust resolution using an external DNSSEC validation tool following propagation. This should be treated as the first remediation action in this report, ahead of any other DNS-dependent finding.

Verification Method.

Confirm via `dig DS caldwellharbortrust.com` that a DS record is now published, and confirm via `delv` or an equivalent DNSSEC-validating resolver query that the zone resolves as “Secure” rather than “Insecure.”

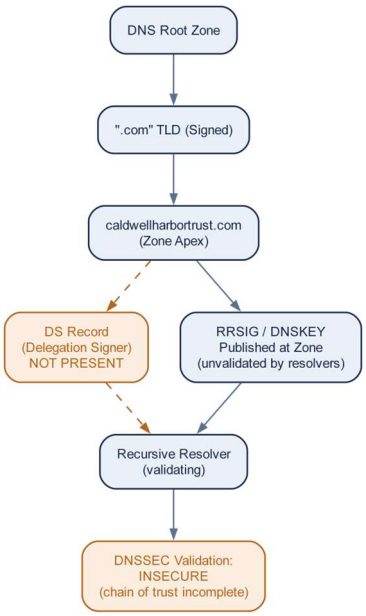

Figure 3 — DNS Trust Chain (DNSSEC)

CS003-02 — MTA-STS Policy Remains in Testing Mode, Providing No Enforcement

Severity	Critical
Category	Transport Security
Reference	RFC 8461 §3

Evidence.

The MTA-STS policy published at mta-sts.caldwellharbortrust.com specifies mode: testing, which instructs sending mail systems to report TLS negotiation failures without actually requiring or enforcing encrypted delivery.

```
$ curl https://mta-sts.caldwellharbortrust.com/.well-known/mta-sts.txt
version: STSv1
mode: testing
mx: mail.caldwellharbortrust.com
max_age: 31536000
```

Technical Analysis.

Interviews with Network Operations confirm the policy was deployed in testing mode intentionally, as a monitoring-first rollout step following RFC 8461's own recommended adoption sequence — but was

never subsequently advanced to mode: enforce, and no one currently owns tracking that transition. As a result, a sending system encountering a TLS downgrade or certificate mismatch when delivering to Caldwell Harbor will report the failure (if TLS-RPT is reviewed — see CS003-04) but will still deliver the message over an insecure or unauthenticated connection rather than refusing delivery.

Business Impact.

Caldwell Harbor's Information Security team believed MTA-STS was providing active protection against TLS interception for correspondent-bank and trust-client correspondence; in its current mode, it provides only visibility, not protection. For a regulated institution handling wire-transfer confirmations, this represents a meaningful gap between the control's intended and actual function.

Recommendation.

Following review of accumulated TLS-RPT data (see CS003-04) to confirm no legitimate correspondent mail system would be blocked by enforcement, advance the policy to mode: enforce. Given the sensitivity of correspondent-banking traffic, Vaixus recommends this transition be prioritized and completed within the current remediation cycle rather than deferred to a future review.

Verification Method.

Confirm via policy fetch that mode: enforce is published, and conduct a controlled trace test simulating a TLS downgrade to confirm delivery is refused rather than falling back to plaintext.

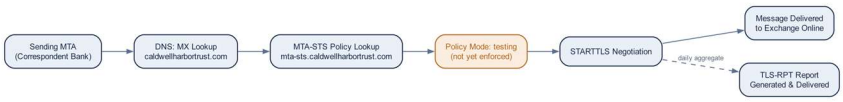

Figure 2 — SMTP Transport Flow (Inbound)

CS003-03 — Reverse DNS Coverage Incomplete Across Outbound Relay IPs

Severity	**High**
Category	Delivery Assurance
Reference	RFC 5321 §Appendix; M3AAWG Sender Best Common Practices

Evidence.

Of six outbound relay IP addresses configured on the Secure Mail Gateway, three lack a matching PTR (reverse DNS) record resolving back to a hostname under caldwellharbortrust.com.

```
$ for ip in 203.0.113.10 203.0.113.11 203.0.113.12 203.0.113.13 203.0.113.14 203.0.113.15;
do dig -x $ip +short; done
mail1.caldwellharbortrust.com.
mail2.caldwellharbortrust.com.
(no result)
(no result)
mail5.caldwellharbortrust.com.
(no result)
```

Technical Analysis.

Several correspondent-bank mail gateways, consistent with common practice in the financial sector, apply strict reverse-DNS validation and silently reject or heavily penalize mail from IP addresses without a resolvable, matching PTR record. Because the Secure Mail Gateway load-balances outbound connections across all six configured IPs, a given message's fate can depend on which of the six IPs happened to be selected for that connection — producing intermittent, difficult-to-diagnose delivery failures to exactly the correspondent-banking counterparties this gateway exists to serve.

Business Impact.

Wire-transfer confirmations and trust-correspondence delivered intermittently, and only to a subset of counterparties, is a difficult failure mode to detect through ordinary monitoring, since the majority of traffic succeeds. This creates a risk of undetected, counterparty-specific communication gaps in exactly the correspondence stream this infrastructure was built to protect.

Recommendation.

Publish matching PTR records for the three affected IP addresses, consistent with the naming pattern already used for the other three relay IPs.

Verification Method.

Confirm via reverse DNS lookup that all six relay IPs resolve to a hostname under caldwellharbortrust.com, and confirm forward-confirmed reverse DNS (FCrDNS) by validating that the hostname's forward A record resolves back to the same IP.

CS003-04 — TLS-RPT Reports Generated but Never Reviewed

Severity	**High**
Category	Operational Risk
Reference	RFC 8460 §3

Evidence.

TLS-RPT is correctly configured and Caldwell Harbor's Secure Mail Gateway vendor has been receiving daily aggregate reports for over a year; however, no Caldwell Harbor employee has an active subscription, dashboard access, or defined review cadence for this data.

```
$ dig TXT _smtp._tls.caldwellharbortrust.com +short
"v=TLSRPTv1; rua=mailto:tlsrpt@securegateway-vendor.example"
```

Technical Analysis.

This finding directly limits the practical value of CS003-02's remediation: the standard-recommended path to safely advancing MTA-STS from testing to enforce mode depends on reviewing TLS-RPT data to confirm no legitimate correspondent would be blocked, and that review has never occurred.

Business Impact.

Caldwell Harbor currently has no visibility into whether any correspondent bank or trust client is already experiencing TLS negotiation failures today — the exact signal needed to safely complete the CS003-02 remediation with confidence.

Recommendation.

Assign a named owner (recommended: Network Operations, in coordination with Information Security) to receive and review TLS-RPT aggregate reports on a defined cadence, beginning immediately and continuing through the MTA-STS enforcement transition.

Verification Method.

Confirm a named recipient has active access to the report mailbox, and confirm at least one documented review cycle occurs prior to the CS003-02 mode transition.

CS003-05 — Secure Mail Gateway Falls Back to Plaintext on STARTTLS Negotiation Failure

Severity	**High**
Category	Transport Security
Reference	RFC 3207 §6

Evidence.

Controlled trace testing of the Secure Mail Gateway's outbound connection behavior shows that when a receiving mail system's STARTTLS negotiation fails or is unavailable, the gateway proceeds to deliver the message over an unencrypted connection rather than deferring delivery.

```
Simulated test: receiving MTA does not advertise STARTTLS
Gateway behavior observed: EHLO -> MAIL FROM -> RCPT TO -> DATA (plaintext)
Expected (per Caldwell Harbor's stated policy intent): connection deferred, retried, or
routed to a fallback secure path
```

Technical Analysis.

This behavior is the outbound counterpart to CS003-02: even once MTA-STS enforcement is enabled for inbound mail (governing what other systems must do to deliver to Caldwell Harbor), the gateway's own outbound behavior independently determines what happens when Caldwell Harbor sends to a correspondent whose system has a TLS problem. Opportunistic fallback-to-plaintext is the historical SMTP default but is inconsistent with the transport-security posture the bank has otherwise invested in.

Business Impact.

A correspondent bank experiencing a temporary certificate or STARTTLS misconfiguration would currently receive Caldwell Harbor's outbound correspondence — potentially including trust or wire-related communication — in plaintext rather than the message being held for secure retry, silently and without any alert to Caldwell Harbor staff.

Recommendation.

Reconfigure the Secure Mail Gateway's outbound delivery policy to defer and retry (rather than deliver in plaintext) when STARTTLS negotiation fails for designated sensitive correspondent domains, with alerting to Network Operations on repeated failure.

Verification Method.

Repeat the simulated STARTTLS-failure trace test post-remediation and confirm the message is deferred rather than delivered in plaintext, and confirm an alert is generated.

CS003-06 — DKIM Key Rotation Overdue

Severity	Medium
Category	Authentication
Reference	RFC 6376 §8.14

Evidence.

The active DKIM selector, chb2024, has been in continuous use for over three years despite its name suggesting an intended annual rotation convention that was not followed after the first year.

```
$ dig TXT chb2024._domainkey.caldwellharbortrust.com +short
v=DKIM1; k=rsa; p=(2048-bit key, in use since original deployment)
```

Technical Analysis.

The 2048-bit key length itself remains adequate by current guidance; the finding is the absence of a followed rotation cadence rather than a weak key. The selector naming convention suggests rotation was originally intended but the process was not operationalized.

Business Impact.

Extended key lifetime increases cryptographic exposure over time and is inconsistent with the rotation discipline expected of a regulated financial institution's security program.

Recommendation.

Generate a new 2048-bit (or stronger) key pair under a new selector, publish it, confirm propagation, and establish an annual rotation calendar reminder to prevent recurrence.

Verification Method.

Confirm new selector via `dig TXT`, confirm DKIM Pass with the new selector in a trace-test Authentication-Results header, and confirm a recurring rotation reminder is scheduled.

CS003-07 — MTA-STS Cache Lifetime Set Long Before Policy Validated in Production

Severity	Medium
Category	Transport Security
Reference	RFC 8461 §3.2

Evidence.

The published MTA-STS policy specifies max_age: 31536000 (one year) while still in testing mode, meaning any sending system that has already cached the policy will continue honoring the long cache lifetime once the policy is changed to enforce mode, slowing real-world uptake of the change.

Technical Analysis.

A long max_age is appropriate for a stable, validated enforce-mode policy, since it reduces unnecessary policy refetches; it is less appropriate during the pre-enforcement testing phase, when Caldwell Harbor may still need to adjust MX hostnames or roll back quickly if an unexpected interoperability issue appears after enabling enforcement.

Business Impact.

If an issue is discovered shortly after transitioning to enforce mode (CS003-02), senders that cached the year-long policy will not see a corrected or rolled-back policy promptly, extending the duration of any resulting delivery disruption.

Recommendation.

Temporarily reduce max_age to a shorter interval (e.g., one week) during the initial enforce-mode rollout window recommended under CS003-02, then increase it back to a longer duration once the transition has been validated as stable.

Verification Method.

Confirm the reduced max_age value is published during the rollout window, and confirm it is increased following a defined stabilization period (recommended: 30 days) with no unresolved delivery issues.

CS003-08 — DMARC Forensic Reporting (RUF) Not Configured

Severity	Medium
Category	Authentication
Reference	RFC 7489 §6.2

Evidence.

Caldwell Harbor's DMARC record specifies an aggregate reporting address (rua) but does not specify a forensic reporting address (ruf).

```
$ dig TXT _dmarc.caldwellharbortrust.com +short
"v=DMARC1; p=reject; pct=100; rua=mailto:dmarc-reports@caldwellharbortrust.com;"
```

Technical Analysis.

Aggregate reports provide statistical summaries of authentication results but do not include the message-level detail (such as source IP and specific header content) that forensic reports can provide for investigating a specific suspected spoofing attempt. Given that regional and community banks are a persistent phishing and business-email-compromise target, message-level detail can meaningfully accelerate incident investigation when a suspicious pattern is first observed in aggregate data.

Business Impact.

Slower investigation of any future spoofing attempt targeting the Caldwell Harbor brand, since aggregate reports alone provide less actionable detail than forensic reports would for a specific suspicious event.

Recommendation.

Add a ruf= address to the DMARC record, directed to a monitored security mailbox, understanding that forensic report volume and recipient support vary by receiving provider and should be evaluated during initial rollout.

Verification Method.

Confirm updated record via `dig TXT`, and confirm receipt of at least one forensic report sample during a controlled test of a deliberately misaligned message.

CS003-09 — No Documented Incident-Response Runbook for Authentication Failures

Severity	**Medium**
Category	Governance
Reference	M3AAWG Sender Best Common Practices

Evidence.

Interviews confirm Caldwell Harbor has a general information-security incident-response program but no specific runbook for responding to a DMARC failure spike, a sudden reputation event, or a suspected domain-spoofing campaign.

Technical Analysis.

Email-authentication incidents have a distinct investigative workflow (aggregate/forensic report review, correlating failure source IPs, coordinating with the Secure Mail Gateway vendor) that a general-purpose incident-response runbook is unlikely to address with sufficient specificity.

Business Impact.

Slower, less consistent response to a future spoofing or reputation incident, at a time (during an active incident) when response speed is most valuable.

Recommendation.

Develop a short, specific runbook covering DMARC failure-spike detection and response, referencing the reporting improvements recommended in CS003-08, and incorporate it into Caldwell Harbor's existing incident-response program.

Verification Method.

Confirm the runbook is documented, reviewed by Information Security, and referenced in the next scheduled incident-response tabletop exercise.

CS003-10 — Secure Mail Gateway Outbound IP Range Adjacency to Previously Flagged Hosting Block

Severity	**Medium**
Category	Reputation Risk
Reference	M3AAWG Sender Best Common Practices

Evidence.

Review of the Secure Mail Gateway's outbound IP allocation shows the block was assigned from a shared hosting provider's range that has, according to public reputation-list history, included IPs flagged for abuse by unrelated tenants in the past 18 months, though none of Caldwell Harbor's specific assigned IPs currently appear on any reputation list.

Technical Analysis.

This is a proximity risk rather than an active reputation problem: shared-range adjacency means a future abuse event by an unrelated tenant on a nearby IP could, in some reputation-scoring systems, marginally affect how conservatively a receiving system treats Caldwell Harbor's own IPs, even without any fault on Caldwell Harbor's part.

Business Impact.

Low current impact, but represents an externality outside Caldwell Harbor's direct control that is worth tracking given the sensitivity of the correspondence this gateway carries.

Recommendation.

Evaluate migrating to a dedicated (non-shared-range) IP allocation for the Secure Mail Gateway during its next infrastructure refresh cycle, or request range-specific reputation monitoring from the current provider in the interim.

Verification Method.

Confirm current IP reputation status via a standard reputation-list check on a recurring (monthly) basis, and revisit dedicated-range migration feasibility at the next infrastructure refresh planning cycle.

CS003-11 — SOA Timing Parameters Are Unreviewed Legacy Defaults

Severity	Low
Category	DNS Hygiene
Reference	RFC 1035 §3.3.13

Evidence.

The zone's SOA record uses refresh, retry, and expire values consistent with an old default BIND template rather than values reviewed for Caldwell Harbor's actual zone change frequency.

```
$ dig SOA caldwellharbortrust.com +short
ns1.dnsprovider.example. admin.caldwellharbortrust.com. 2019031201 86400 7200 3600000
172800
```

Technical Analysis.

The serial number format indicates the record has not been substantively reviewed since at least 2019, though the zone itself has clearly been updated many times since (reflected in DNS content changes, not necessarily the SOA timing values themselves). This is a low-severity hygiene item rather than an active problem.

Business Impact.

Minimal current impact; primarily relevant if Caldwell Harbor ever needs rapid secondary-nameserver propagation during an incident, where legacy refresh/retry intervals could slow convergence.

Recommendation.

Review and update SOA timing parameters to current best-practice values appropriate for a zone with regular administrative changes.

Verification Method.

Confirm updated SOA values via `dig SOA` following the change.

CS003-12 — DNS TXT Records Reference Bank's Pre-Rebrand Legacy Name

Severity	Low
Category	DNS Hygiene
Reference	General DNS Hygiene

Evidence.

Several historical domain-verification TXT records at the zone apex reference “Caldwell Harbor Savings”, the institution's name prior to a rebrand completed several years ago, rather than its current name.

Technical Analysis.

These records are almost certainly inactive verification artifacts from long-decommissioned third-party services and pose no functional risk, but their presence is a minor documentation-hygiene issue that complicates zone auditing.

Business Impact.

No functional impact; a minor auditability concern only.

Recommendation.

Review each legacy TXT record to confirm the associated third-party service is no longer in use, and remove confirmed-inactive records during the next scheduled zone cleanup.

Verification Method.

Confirm via `dig TXT` that legacy records have been removed following review, with no unexpected loss of active third-party verification.

CS003-13 — BIMI Not Implemented Despite Satisfied DMARC Prerequisite

Severity	Informational
Category	Security Best Practices
Reference	BIMI Group Specification

Evidence.

No BIMI record exists at default._bimi.caldwellharbortrust.com, despite Caldwell Harbor's DMARC policy already being enforced at p=reject — the enforcement level BIMI requires as a prerequisite.

Technical Analysis.

Unlike the other environments in Vaixus's portfolio, Caldwell Harbor's DMARC posture already satisfies BIMI's core prerequisite. This is therefore a genuine, immediately actionable opportunity rather than a future-state item contingent on other remediation.

Business Impact.

No current negative impact; recorded as a positive-opportunity item given the bank's brand-trust interest in a regulated, correspondent-facing context.

Recommendation.

Evaluate BIMI implementation, including obtaining a Verified Mark Certificate (VMC) if logo display in supporting mailbox providers (e.g., Gmail) is desired, in coordination with Marketing and Brand teams.

Verification Method.

No verification required at this time; revisit as an optional enhancement following completion of the Critical and High findings in this report.

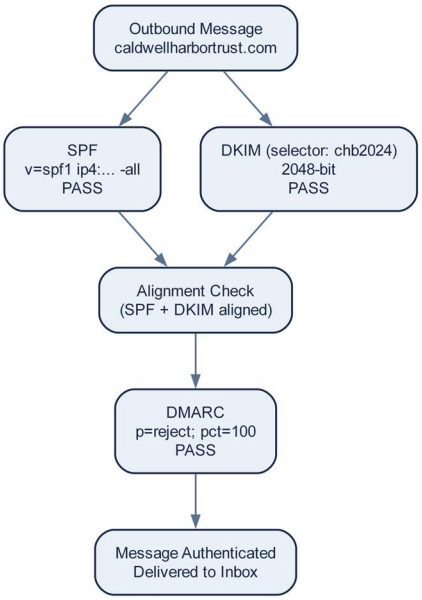

Figure 4 — Authentication Architecture (Outbound)

8. Risk Prioritization

Findings are prioritized below by severity and remediation effort, establishing the sequencing basis for the Remediation Strategy in Section 10.

Priority	Finding ID	Severity	Effort	Rationale
1	CS003-01	Critical	Low	Single registrar action (DS record submission); underlies every other control
2	CS003-04	High	Low	Must precede CS003-02 to safely validate enforcement readiness
3	CS003-02	Critical	Medium	Highest-impact transport control; depends on CS003-04 data review
4	CS003-07	Medium	Low	Bundled with CS003-02 rollout
5	CS003-03	High	Low	Three DNS record additions
6	CS003-05	High	Medium	Requires Secure Mail Gateway policy reconfiguration
7	CS003-06	Medium	Low	Standard key rotation procedure
8	CS003-08	Medium	Low	Single DNS record edit
9	CS003-09	Medium	Medium	Requires runbook authoring and IR program integration

Priority	Finding ID	Severity	Effort	Rationale
10	CS003-10	Medium	Medium	Contingent on infrastructure refresh timing
11	CS003-11	Low	Low	Single DNS record update
12	CS003-12	Low	Low	Zone cleanup during next scheduled review
13	CS003-13	Informational	Medium	Optional enhancement; not required for remediation completion

9. Business Impact Analysis

Foundational Trust Integrity

CS003-01 is the keystone finding in this report: because DNSSEC's chain of trust is incomplete, every other DNS-published control examined here — SPF, DKIM, DMARC, and MTA-STS records alike — is retrieved by receiving systems through an unvalidated resolution path. Remediating this finding does not by itself fix any other control, but it is the precondition for the integrity guarantee Caldwell Harbor's broader authentication investment is intended to provide.

Transport Security Gap Between Intent and Reality

CS003-02 and CS003-05 together show that Caldwell Harbor's transport-security controls are not yet providing the protection its Information Security team believes they provide, in both the inbound (MTA-STS testing mode) and outbound (plaintext fallback) direction. This is a materially different risk profile than “no transport security control exists,” but the gap between perceived and actual protection is itself a risk that this report's remediation program directly closes.

Correspondent-Banking Delivery Assurance

CS003-03 and CS003-04 together limit Caldwell Harbor's visibility into whether its correspondence with correspondent banks and trust clients is reliably reaching its destination today, which is a foundational concern for an institution whose infrastructure exists specifically to serve that correspondence reliably and securely.

10. Remediation Strategy

Remediation is organized into three phases sequenced by dependency and regulatory sensitivity.

Phase 1 — Immediate (Weeks 1–2)

Action	Addresses	Expected Result	Operational Considerations
Submit DS record to registrar to complete DNSSEC chain of trust	CS003-01	Zone validates as Secure end-to-end	Coordinate with registrar; propagation may take up to 48 hours

Action	Addresses	Expected Result	Operational Considerations
Assign named owner to TLS-RPT review; begin active monitoring	CS003-04	Baseline visibility into TLS negotiation failures established	Prerequisite for CS003-02 rollout
Publish missing PTR records for 3 outbound relay IPs	CS003-03	Full reverse DNS coverage across all relay IPs	DNS-only change

Phase 2 — Near-Term (Weeks 3–6)

Action	Addresses	Expected Result	Operational Considerations
Reduce MTA-STS max_age; transition policy to enforce mode	CS003-02, CS003-07	Active TLS enforcement for inbound correspondent mail	Contingent on clean TLS-RPT data from Phase 1
Reconfigure Secure Mail Gateway to defer rather than fall back to plaintext	CS003-05	No outbound correspondence delivered unencrypted	Requires gateway vendor coordination
Rotate DKIM key under new selector	CS003-06	Current key-age hygiene restored	Brief dual-key overlap period recommended
Add ruf= forensic reporting address to DMARC record	CS003-08	Message-level detail available for incident investigation	DNS-only change

Phase 3 — Governance and Hygiene (Weeks 7–12)

Action	Addresses	Expected Result	Operational Considerations
Author and adopt DMARC-failure incident-response runbook	CS003-09	Faster, consistent response to future authentication incidents	Incorporate into existing IR program
Evaluate dedicated IP allocation for Secure Mail Gateway	CS003-10	Reduced shared-range reputation exposure	Contingent on infrastructure refresh cycle
Review and update SOA timing parameters; clean up legacy TXT records	CS003-11, CS003-12	Improved zone hygiene and auditability	Low risk; schedule with other DNS maintenance
Evaluate BIMI implementation	CS003-13	Brand logo display in supporting inboxes	Optional; coordinate with Marketing/Brand

11. Verification Plan

Finding	Verification Method	Success Criterion
CS003-01	DS record lookup + external DNSSEC validator	Zone validates as “Secure” end-to-end
CS003-02 / CS003-07	MTA-STS policy fetch + simulated downgrade trace test	mode: enforce published; downgrade attempt refused, not delivered
CS003-03	Reverse DNS lookup across all six relay IPs	All IPs resolve to a matching, forward-confirmed hostname
CS003-04	TLS-RPT recipient access + review-log confirmation	Named owner has access; at least one documented review completed
CS003-05	Simulated STARTTLS failure trace test	Message deferred, not delivered in plaintext
CS003-06	DKIM selector trace test	New selector referenced with Pass result
CS003-08	DMARC record inspection + forensic report test	ruf= present; sample forensic report received
CS003-09	Runbook document review	Runbook documented and referenced in IR program
CS003-10	Monthly reputation-list check	No adverse listing; migration plan documented
CS003-11 / CS003-12	SOA and TXT record inspection	Updated SOA values; legacy records removed

12. Final Assessment

Caldwell Harbor Trust's email security posture reflects an organization that has made genuine, above-average investment in transport-security and authentication controls relative to Vaixus's broader portfolio — DMARC enforcement, MTA-STS, TLS-RPT, and DNSSEC signing infrastructure are all present in some form. The findings in this report concentrate on completing and operationalizing controls that were correctly selected but not fully finished or monitored, rather than on foundational gaps in security strategy.

Vaixus rates Caldwell Harbor's current infrastructure maturity as Managed (Level 3 of 5 on Vaixus's internal maturity scale), meaningfully ahead of the other environments in this portfolio, with a clear and achievable path to Optimized (Level 5) once the two Critical findings and their closely dependent High findings (CS003-03, CS003-04, CS003-05) are resolved.

No finding in this report indicates active compromise or an exploited vulnerability. Every finding reflects a control that was correctly chosen but incompletely deployed or insufficiently monitored — a distinct and more advanced starting point than the earlier-stage organizations elsewhere in this portfolio, and one that is fully remediable within the twelve-week program outlined above.

13. References

- RFC 1035 — Domain Names — Implementation and Specification
- RFC 3207 — SMTP Service Extension for Secure SMTP over Transport Layer Security
- RFC 4033 — DNS Security Introduction and Requirements
- RFC 4035 — Protocol Modifications for the DNS Security Extensions
- RFC 6376 — DomainKeys Identified Mail (DKIM) Signatures
- RFC 7489 — Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- RFC 8460 — SMTP TLS Reporting
- RFC 8461 — SMTP MTA Strict Transport Security (MTA-STS)
- M3AAWG Sender Best Common Practices, Messaging, Malware and Mobile Anti-Abuse Working Group
- BIMI Group — Brand Indicators for Message Identification Specification

14. Technical Appendix

A. Full DNS Record Set (Synthetic Laboratory Environment)

caldwellharbortrust.com

Record Type	Name	Value
MX	@	10 mail.caldwellharbortrust.com
TXT (SPF)	@	v=spf1 ip4:203.0.113.10/29 -all
TXT (DKIM)	chb2024._domainkey	v=DKIM1; k=rsa; p=(2048-bit key, unrotated 3+ years — see CS003-06)
TXT (DMARC)	_dmarc	v=DMARC1; p=reject; pct=100; rua=mailto:dmarc-reports@caldwellharbortrust.com; (no ruf — see CS003-08)
TXT (MTA-STS policy)	mta-sts	mode: testing; max_age: 31536000 (see CS003-02, CS003-07)
TXT (TLS-RPT)	_smtp._tls	v=TLSRPTv1; rua=mailto:tlsrpt@securegateway-vendor.example
DS	@	Not present at registrar (see CS003-01)
DNSKEY / RRSIG	@	Present at zone; unvalidatable without DS (see CS003-01)
SOA	@	Legacy timing defaults, serial dated 2019 (see CS003-11)

Outbound Relay IP / PTR Coverage

IP Address	PTR Record	Status
203.0.113.10	mail1.caldwellharbortrust.com	Present
203.0.113.11	mail2.caldwellharbortrust.com	Present
203.0.113.12	(none)	Missing — see CS003-03
203.0.113.13	(none)	Missing — see CS003-03
203.0.113.14	mail5.caldwellharbortrust.com	Present
203.0.113.15	(none)	Missing — see CS003-03

B. Sample SMTP Trace — Outbound STARTTLS Failure Fallback

```
220 correspondent-mta.example ESMTP
EHLO mail.caldwellharbortrust.com
250-correspondent-mta.example
250 SIZE 52428800
; NOTE: no STARTTLS advertised by receiving system
MAIL FROM:<ops@caldwellharbortrust.com>
250 OK
RCPT TO:<wires@correspondent-bank.example>
250 OK
DATA
; message transmitted in plaintext — see CS003-05
```

C. Command Output — DNSSEC Validation (Post-Remediation, Simulated)

```
$ delv @8.8.8.8 caldwellharbortrust.com
; fully validated
caldwellharbortrust.com. 3600 IN A 203.0.113.20
; validated with proof of insecurity for delegation from com to caldwellharbortrust.com:
no; fully secure
```

D. Vendor / Control Inventory

Control / Vendor	Role	Configuration State	Admin Owner
Microsoft 365	Corporate mailboxes	Standard configuration	IT Operations
Secure Mail Gateway (on-prem)	Compliance journaling; correspondent TLS enforcement	Plaintext fallback enabled (see CS003-05)	Network Operations
DNSSEC	Zone signing	Signed at zone; DS record missing (see CS003-01)	Network Operations
MTA-STS	Inbound transport policy	Testing mode (see CS003-02)	Information Security

Control / Vendor	Role	Configuration State	Admin Owner
TLS-RPT	Transport reporting	Configured; unreviewed (see CS003-04)	Unassigned
DMARC	Sender authentication policy	Enforced (p=reject); no RUF (see CS003-08)	Information Security
Managed DNS Provider	Authoritative DNS hosting	Standard configuration	Network Operations